C13

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/076,652	03/10/2005	Steven D. Tonnesen	ION1200-1	6276

44654 7590 01/25/2008

SPRINKLE IP LAW GROUP
1301 W. 25TH STREET
SUITE 408
AUSTIN, TX 78705

EXAMINER
NOONAN, WILLOW W

ART UNIT	PAPER NUMBER
2146	

MAIL DATE	DELIVERY MODE
01/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/076,652	TONNESEN, STEVEN D.	
	Examiner	Art Unit	
	Willow Noonan	2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :10/14/2005, 8/13/2007, 12/20/2007.

DETAILED ACTION

1. The instant application having Application No. 11/076,652 has a total of 8 claims pending in the application; there is 1 independent claims and 7 dependent claims, all of which are ready for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

Drawings

3. The applicant's drawings submitted are acceptable for examination purposes.

Information Disclosure Statement

4. As required by M.P.E.P. 609(C), the applicant's submissions of the Information Disclosure Statements dated October 14, 2005, August 13, 2007 and December 20, 2007 are acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending. As required by M.P.E.P 609 C(2), a copy of the PTOL-1449 initialed and dated by the examiner is attached to the instant office action.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "a second network interface coupled to the processor," but it is not clear how this element is used in or incorporated into the system. Appropriate clarification and description are required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper (U.S. Patent No. 7,272,646).

Regarding claims 1 and 2, Cooper teaches a system for detecting aberrant network behavior by clients of a network access gateway, comprising a processor; a first network interface coupled to the processor; a storage media accessible by the processor. *See generally* Cooper at col. 7-8, *System Overview*. Cooper teaches that

the system may observe a network communication received at the first network interface and determine if the network communication is aberrant. *See* Cooper at col. 3, lines 46-55 ("The monitoring system listens on a network, logs events, and takes action, all in accordance with a rule based system-wide policy"). Cooper further teaches, if the network communication is determined to be aberrant, record the event to storage and perform notifications to a registered entity. *See* Cooper at col. 4, paragraph 3 ("The event's disposition determines whether the event is allowed, i.e. conforms to the specified policy or disallowed and what action, if any, should be taken by a system monitor in response to that event. Possible actions include, for example, logging the information into a database, notifying a human operator, and disrupting the offending network traffic.").

Although Cooper only explicitly teaches monitoring one network interface, it would be obvious to one of ordinary skill to monitory a second network interface. There is always a general motivation to extend a device operable in a single domain so that the device may operate in a plurality of domains.

Regarding claim 3, Cooper teaches that the computer instructions are further operable to observe the network communication regardless of protocol. *See* Cooper at col. 19, lines 2-11 ("The preferred embodiment provides a streams-based network monitor that can be run in a standalone mode independent of the policy monitor. In this way it can be used to provide a detailed, streams-based view of the network traffic, or a subset thereof. For example, run in standalone mode is desirable when a particular

protocol is not supported natively by the policy monitor and an end user desires to see raw data to gain an understanding of what is going on").

Regarding claims 4 and 5, Cooper teaches associating the client with an identifier. *See* Cooper at col. 6, *Table A* ("Credential: An identification of the initiator or target of a protocol event at a particular protocol level. For lower-level protocols, credentials are, for example, IP addresses or UDP port numbers").

Regarding claims 6 and 7, Cooper teaches that the system may receive at least one configuration adjustment from an internal or external source of the system. *See* Cooper at col. 8, *Policy Generator*.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper in view of Porras (U.S. Patent No. 6,708,212).

Regarding claim 8, Porras teaches that the system may determine if a client's network communication is aberrant by means of communication with a suspicion accumulator. *See* Poras, *Abstract* ("A method of network surveillance includes receiving network packets handled by a network entity and building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. A comparison of the statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity"). It would have been obvious to one of ordinary skill in the art to use Porras' technique in Cooper's system because both disclosures relate to network monitoring and threat/problem detection.

Conclusion

10. Please see the included *Notice of References Cited* for additional prior art considered pertinent to applicant's disclosure but not explicitly relied upon in this action.

11. The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line no(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application.

12. When responding to this office action, Applicant is advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Willow Noonan whose telephone number is (571) 270-1322. The examiner can normally be reached on Monday through Friday, 7:30 AM-5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

William Norman

JEFFREY PWU
SUPERVISORY PATENT EXAMINER

PTO/SB/08A (04-03)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	11/076,652
				Filing Date	March 10, 2005
				First Named Inventor	Steven D. Tonnesen
				Group Art Unit	2146
				Examiner Name	Noonan, Willow W.
Sheet	1	of	2	Attorney Docket Number	ION1200-1

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number		Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear
		Number	Kind Code (if known)			
/WWN/	A1	2003/0212800	A1	11/13/2003	Jones et al.	
	A2	2002/0029260	A1	03/07/2002	Dobbins et al.	
	A3	2003/0069956	A1	04/10/2003	Gleseke et al.	
	A4	2003/0163603	A1	08/28/2003	Fry et al.	
	A5	2003/0177477	A1	09/18/2003	Fuchs	
/WWN/	A6	2004/0268234	A1	12/30/2004	Sampathkumar et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Country Code	Number	Kind Code (if known)	Publication Date MM-DD-YYYY (Number 43)	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines Where Relevant Passages or Figures Appear

Examiner Signature	/Willow Noonan/	Date Considered	01/21/2008